

## Data Privacy Policy for Employees

- ◆ Hastings (Westport) Ltd t/a Hastings Insurance Brokers, Irishweddinginsurance.ie & Mytravelinsurance.ie;
- ◆ David Flannelly (Holdings) Ltd t/a Hastings Insurance Brokers & Flannelly Insurances;
- ◆ Pat Hardiman Insurances Ltd t/a Hastings Insurance Brokers and
- ◆ Burke Insurances Ltd t/a Hastings Insurance Brokers

*thereafter referred to as 'Hastings', (the Limited Company).*

### 1 Introduction

We are committed to safeguarding the privacy of the personal data that we gather concerning our employees (“**you**” or “**employees**”) for management, human resources and payroll purposes.

As a Hastings employee, you understand and acknowledge that we collect, use and disclose your personal data in accordance with this Privacy Policy for Employees (this “**Policy**”).

### 2 The Application of this Policy

This Policy applies to employees’ personal data and to the use of that personal data in any form – whether oral, electronic or written.

This Policy gives effect to Hastings commitment to protect your personal data. Your personal data will be processed by Hastings, the entity with which you have an employment relationship with for the purposes set out in Section 4 below. Your personal data may be disclosed where necessary for human resources administration purposes.

### 3 The Types of Personal Information We Process

The term “**personal data**” in this Policy refers to information that does or is capable of identifying you as an individual. The types of personal data that we process include:

- name, gender, home address and telephone number/mobile telephone number, date of birth, marital status, emergency contacts/next of kin;
- residency and work permit status, nationality and passport information, where applicable ;
- CV, interview notes;
- PRSI number or other taxpayer identification number, banking details;
- sick pay, pensions, insurance and other benefits information (including the gender, age, nationality);
- date of employment, date(s) of promotions(s), work history, technical skills, educational background, professional certifications and registrations, training courses attended or any training undertaken including CPD carried out;
- clothing sizes, photograph, physical limitations and special needs;
- records of work absences including sickness leave/medical certs, maternity leave, parental leave, force majeure leave, carers leave, unauthorised absence, holiday entitlement and requests, salary history and expectations, job description, induction programmes, performance appraisals, and disciplinary and grievance procedures (including monitoring compliance with and enforcing Hastings policies);
- where permitted by law and proportionate in view of the function to be carried out by an employee the results of credit and criminal background checks, health certifications, driving licence number, vehicle registration and driving history;
- information required to comply with laws, the requests and directions of law enforcement authorities or court orders (e.g., child support or debt payment information);
- personal data of family members who are named on any policy concerning health and dental health where payment is made through your salary;
- acknowledgements regarding Hastings policies, including the employee handbook, any compliance based policy, computer and other corporate resource usage policies;
- information captured on telephone recordings and other technology systems, to the extent permitted by applicable law;

- voicemails, emails, correspondence and other communications created, stored or transmitted by an employee using Hastings computer or communications equipment (although correspondence exchanged using Hastings equipment but using personal addresses is only processed to the extent permitted by applicable law);
- date of resignation or termination, reason for resignation or termination, information relating to administering termination of employment (*e.g.*, references);
- details of next of kin, provided in the event of an emergency;
- any other relevant data that could be necessary to comply with Hastings record keeping purposes.

#### **4 Legal Basis for Processing**

The legal basis we rely on for collecting your personal data is the formation of a contract between you and Hastings. The processing of your personal data is necessary for the performance of your contract during the duration of your employment. Most of the personal data we process is information that you knowingly provide to us. However, in other instances, we process personal data that we are able to infer about you based on other information you provide to us or during our interactions with you, or personal data about you that we receive from a third party using a process that we have told you about. There may be instances in which the personal data that you provide to us or we collect is considered Sensitive Personal Data. “Sensitive Personal Data” is personal data from which we can determine or infer an individual’s racial or ethnic origin, political opinions, religious beliefs or other beliefs of a similar nature, membership in a trade union or professional association, physical or mental health or condition, genetic data, sexual life or judicial data (including information concerning criminal offences). Your explicit consent will be sought before processing begins unless the processing is authorised by law, *ie.* to protect your interests, to comply with employment legislation or for reasons of public interest.

#### **5 How We Use Personal Information**

We may collect, use and disclose personal data concerning employees in order to:

- evaluate applications for employment;
- manage all aspects of an employee’s employment relationship, including, but not limited to, payroll, benefits, corporate travel and other reimbursable expenses, development and training, absence monitoring, performance appraisal, disciplinary and grievance processes and other general administrative and human resource-related processes;
- develop manpower and succession plans;
- maintain sickness records;
- investigate and respond to claims against Hastings, its staff and clients;
- administer termination of employment and provide and maintain references;
- maintain emergency contact and health details (which involves Hastings holding information on those you nominate on any health or dental policy).

We may also utilise “Secret Shopper” programs, to monitor the quality of our customer service.

We may monitor Internet use and communications in accordance with applicable laws and Hastings Policy on use of Information Technology Resources as set out in the Hastings Employment Policies and Procedures Handbook.

We may retain certain personal data of employees after their employment ends for any residual aspect of the purposes set out above. We will only retain such personal data for as long as it is necessary and in all cases for no longer than permitted by Hastings Records Management Policy.

Unless otherwise stated, all personal data we request from you is obligatory. If you do not provide and/or allow us to process all obligatory personal data as requested, we will not be able to keep complete information about you, thus affecting our ability to accomplish the purposes set out above

#### **6 Disclosures of Your Personal Data**

##### **6.1 General**

In order to carry out the purposes outlined above, information about you will be disclosed for the purposes set out above to the human resources department, line managers, consultants, advisers and other appropriate persons within the Group.

## **6.2 Our Agents, Service Providers and Suppliers**

Like many businesses, from time to time, we outsource the processing of certain functions and/or information to third parties. When we do outsource the processing of your personal data to third parties or provide your personal data to third-party service providers, we oblige those third parties to protect your personal data in accordance with the terms and conditions of this Policy, with appropriate security measures.

## **6.3 Business Transfers**

As we continue to develop our business, we may buy or sell other brokerages. In such transactions, employee information is generally one of the transferred business assets and we may include your personal data as an asset in any such transfer. Also, in the unlikely event that we, or substantially all of our assets, are acquired, employee information may be one of the transferred assets.

## **6.4 Legal Requirements**

We reserve the right to disclose any personal data we have concerning you if we are compelled to do so by a court of law or requested to do so by a governmental entity or if we determine it is necessary or desirable to comply with the law or to protect or defend our rights or property in accordance with applicable laws. We also reserve the right to retain personal data collected and to process such personal data to comply with accounting, tax rules, regulations and any specific record retention laws.

## **7 Updating or Accessing Your Personal Data**

With some limited exceptions, you may request a copy of personal data we hold/maintain about you by submitting a written request by email to the HR Department. We may not disclose data that you are not entitled to receive (*e.g.*, data revealing information about another individual). You may request that we correct, delete or stop processing, personal data that we hold about you on legitimate grounds by sending an email to the HR Department. If we agree that the information is incorrect, or that the processing should be stopped, we will delete or correct the information. If we do not agree that the information is incorrect, we will tell you that we do not agree and record the fact that you consider that information to be incorrect. You may also request your personal data we hold be transferred to another organisation.

## **8 Protecting Your Personal Information**

The personal data we collect from you is stored by us and/or our service providers on databases protected through a combination of physical and electronic access controls, firewall technology and other reasonable security measures. Nevertheless, such security measures cannot prevent all loss, misuse or alteration of personal data and we are not responsible for any damages or liabilities relating to any such incidents or the fullest extent permitted by law. Where required under law, we will notify you of any such loss, misuse or alteration of personal data that may affect you, so that you can take the appropriate actions for the due protection of your rights.

## **9 Changes to this Policy**

Just as our business changes constantly, this Policy may also change. To assist you, this Policy has an effective date set out at the end of this document.

## **10 Request for Access to Personal Information / Questions or Complaints**

If you have any questions about this Policy, about the processing of your personal data as described herein, or any concerns or complaints with regard to the administration of the Policy, please contact [Dataprotection@hastings.ie](mailto:Dataprotection@hastings.ie) or if you would like to submit a request (in the manner described in Section 7 above) for access to the personal data that we maintain about you, please contact the HR Department.

Effective Date: 19/04/2021